



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/080,647	02/22/2002	Eiichi Horita	10746/31	8170
26646	7590	03/31/2006		
KENYON & KENYON LLP ONE BROADWAY NEW YORK, NY 10004			EXAMINER HENEGHAN, MATTHEW E	
			ART UNIT	PAPER NUMBER
			2134	
DATE MAILED: 03/31/2006				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/080,647	Applicant(s) HORITA ET AL.	
	Examiner Matthew Heneghan	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 January 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3,4,6,7,9,10 and 12-26 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 26 is/are allowed.
- 6) ☒ Claim(s) 1,3,4,6,7,9,10 and 12-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 23 January 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>4/2/02</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. In response to the previous office action, Applicant has amended claims 1, 3, 4, 7, 10, and 13-20; added claims 21-26; and cancelled claims 2, 5, 8, and 11. Claims 1, 3, 4, 6, 7, 9, 10, and 12-26 have been examined.

Information Disclosure Statement

2. In view of Applicant's comments (see Remarks, filed 23 January 2006, p. 22), the following Information Disclosure Statement in the instant application has been fully reconsidered:

IDS filed 2 April 2002.

Drawings

3. The drawings were received on 23 January 2006. These drawings are acceptable.

Specification

4. The incorporation of essential material in the specification by reference to an unpublished U.S. application, foreign application or patent, or to a publication is

Art Unit: 2134

improper. Applicant is required to amend the disclosure to include the material incorporated by reference, if the material is relied upon to overcome any objection, rejection, or other requirement imposed by the Office. The amendment must be accompanied by a statement executed by the applicant, or a practitioner representing the applicant, stating that the material being inserted is the material previously incorporated by reference and that the amendment contains no new matter. 37 CFR 1.57(f).

The specification describes the generation of partial digital signatures in the absence of a trusted third party simply by referencing a publication by Boneh et al. (see Specification, page 20, lines 8-14). This material is essential to the claimed invention and must be explicitly described in the disclosure.

Claim Objections

5. Claims 7, 10, and 15-20 are objected to because of the following informalities: They lack transitional phrases. For purposes of the prior art, it is being presumed that each limitation is being recited in an open-ended manner, beginning after the first instance of the word "wherein." Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Art Unit: 2134

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 21-25 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claimed invention is a program that does not have a concrete and tangible output.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1, 3, 7, 9, 13, 15, 17, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malkin, Michael et al. "Building Intrusion Tolerant Applications," Darpa Information Survivability Conference and Exposition, 2000 in view of U.S. Patent No. 4,405,829 to Rivest et al.

As per claims 1, 7, 13, 15, 17, and 19, Malkin discloses a system wherein a set of servers select a partial signature key based upon the client's specification, thereby obviating the need for a trusted third party. Each uses a hash derived from the partial signature key to sign a message (i.e. a document), and sends back the computed

Art Unit: 2134

partial signature (see Sections 3.1 and 4). The signatures are combined when a t-out-of-k threshold is reached, producing a combined signature (see Section 3.1.1).

Malkin does not disclose a signature key generating algorithm using an LCM function.

Rivest discloses a signature key generating algorithm (RSA) that uses the LCM function in generating a key from the arguments (see column 5, lines 9-12), and suggests that this algorithm allows for the usage of public keys in signature generation (see column 3, lines 64-68).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Malkin by using the algorithm of Rivest for signature generation, as this allows for the usage of public keys in signature generation.

As per claims 3 and 9, a mechanism is disclosed to identify corrupted signatures sent by servers (see section 4.1).

8. Claims 4, 6, 10, 12, 14, 16, 18, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malkin, Michael et al. "Building Intrusion Tolerant Applications," Darpa Information Survivability Conference and Exposition, 2000 in view of U.S. Patent No. 4,405,829 to Rivest et al. as applied to claim 1 et al. above, and further in view of U.S. Patent No. 5,610,982 to Micali.

Malkin and Rivest only disclose the passing of the computed partial signature by the server, not suggesting to also pass the document.

Micali discloses the passing of the document with a certificate having the signature, and suggests that this keeps the members accountable for the certificates they cause to issue (see column 9, lines 40-63).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Malkin and Rivest by passing the document with the signature, as disclosed by Micali, as this keeps the members accountable for the certificates they cause to issue.

Allowable Subject Matter

9. Claim 26 is allowed.

10. Claims 21-25 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 101, set forth in this Office action.

11. The following is a statement of reasons for the indication of allowable subject matter:

Each of the independent claims recites a partial digital signature number set selecting step that is not disclosed by the previously cited references. No art could be found that would render it obvious to choose the claimed set.

Each of the dependent claims would be allowable based upon their dependence upon an allowable claim.

Response to Arguments

12. Regarding Applicant's traversal of the objection to the specification, the sections of the specification upon which Applicant relies upon for number generation both incorporate by reference non-patent literature to support this function (Wu et al. and Boneh et al.). The algorithm for number generation is essential to the invention and therefore must be explicitly described in the specification.

13. Regarding Applicant's traversal of the objections to claims 7, 10, and 15-20, "wherein" is not an acceptable transitional phrase. See MPEP 2111.03.

14. In response to applicant's argument that the references (particularly Rivest) fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., using particular variables for the "predetermined values") are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Rivest discloses a transformation number (the key) for the transformation process (signature generation) derived from a least common multiple of predetermined values (i.e. p and q). The modification of Rivest teaches to Applicant's invention insofar as it is claimed.

Conclusion

15. Applicant's amendment necessitated the new grounds of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques, can be reached at (571) 272-6962.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks

Art Unit: 2134

P.O. Box 1450
Alexandria, VA 22313-1450

Or faxed to:
(571) 273-3800

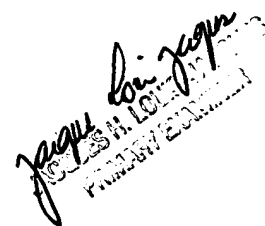
Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MEH



March 28, 2006



Handwritten signature and stamp, likely indicating a filing or processing date.